REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 27-04-2007	**2. REPORT TYPE** FINAL REPORT	**3. DATES COVERED** *(From - To)* JULY 2006 to JULY 2007

4. TITLE AND SUBTITLE
Coast Guard AHLTA Technology Business Case Analysis

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
FREESE, MARK, R, CAPT, USPHS, DENT

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
TRICARE Management Activity, OASD(HA)
Skyline 5, Suite 810A, 5111 Leesburg Pike
Falls Church, VA 22041

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
US Army Medical Department Center and School
BLDG 2841 MCCS-HFB (Army-Baylor Program in Health and Business Administration)
3151 Scott Road, Suite 1411
Fort Sam Houston, TX 78234-6135

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
30-07

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Coast Guard must deliver AHLTA to its clinics, either through direct connection to military treatment facilities (MTFs), making the clinics satellite clinics, or through developing their own servers at the Operational Service Center (OSC) complex in Martinsburg. The Coast Guard Telecommunications & Information Systems Command (TISCOM) has made it clear that any system connecting to the Department of Defense (DOD) network may not connect to the Coast Guard Data Network (CGDN+), and the DOD has made a similar policy. Thus connecting to AHLTA via MTFs would entail an entire secondary network be established at each clinic site, one DOD and one CGDN+. This would be a major cost driver, far surpassing the costs associated with developing a Coast Guard AHLTA server farm at the OSC. Unless any of the assumptions undergo change, this analysis demonstrates that the Coast Guard would be better served by establishing their own AHLTA servers at the OSC center at Martinsburg, West Virginia versus connecting directly to MTFs. The net present value (cost) differential of this route results in a savings of $6,633,152 to the Coast Guard.

15. SUBJECT TERMS
AHLTA, Coast Guard, CGDN+, Operational Service Center, DOD

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Education Technician
U	U	U	UU	39	**19b. TELEPHONE NUMBER** *(Include area code)* (210) 221-6443

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE. Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

4. TITLE. Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER. Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER. Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER. Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER. Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER. Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

Army-Baylor University

Graduate Program in Health and Business Administration

Coast Guard AHLTA Technology Business Case Analysis

A Graduate Management Project Submitted in Partial Fulfillment of Requirements for the

Degree of Master's in Health Administration

27 April 2007

By

Captain Mark R. Freese

Administrative Resident, TRICARE Management Activity

5111 Leesburg Pike, Skyline 5, Suite 810

Falls Church, VA 22041

Acknowledgements

I would like to thank Mr. Pradeep Gidwani, the Acting Chief of Staff for the Deputy Director and Program Executive Officer of the TRICARE Management Activity (TMA), Office of the Assistant Secretary of Defense (Health Affairs). Mr. Gidwani was instrumental in allowing access to the directorates of TMA. In a similar vein, I would like to extend my deepest appreciation to CAPT Sharon Ludwig, the Chief, Health Systems and Management Division (CG-1123) who opened the resources of the Coast Guard to my study. I also would like to acknowledge LTC Marsha Patrick, who was able to add guidance even though she was half a world away.

Disclaimer

This analysis provides approximations of important financial consequences that should be considered in decisions involving the purchase, installation, and configuration of computing hardware and software. The analysis is based on information, which was provided by TMA, the U S Coast Guard and their contractors. However, any opinions express herein are those solely of the author and do not necessarily agree with those of the Department of Defense or the Department of Homeland Security, nor those of any employees or contractors of those departments.

Executive Summary

U. S. Coast Guard (USCG) command (CG-11) has determined due to Executive Orders that it must be running AHLTA as soon as feasible, with 2008 as the goal. Currently the USCG is utilizing the Composite Health Care System (CHCS). Two scenarios are investigated in this analysis: The Coast Guard must therefore deliver AHLTA to its clinics, either through direct connection to military treatment facilities (MTFs), making the clinics satellite clinics, or through developing their own servers at the Operational Service Center (OSC) complex in Martinsburg.

The Coast Guard Telecommunications & Information Systems Command (TISCOM) has made it clear that any system connecting to the Department of Defense (DOD) network may not connect to the Coast Guard Data Network (CGDN+), and the DOD has made a similar policy. Thus connecting to AHLTA via MTFs would entail an entire secondary network be established at each clinic site, one DOD and one CGDN+. This would be a major cost driver, far surpassing the costs associated with developing a Coast Guard AHLTA server farm at the OSC. Unless any of the assumptions undergo a drastic change, this analysis demonstrates that the Coast Guard would be better served by establishing their own AHLTA servers at the OSC center at Martinsburg, West Virginia versus connecting directly to MTFs. The net present value (cost) differential of this route results in a savings of $6,633,152 to the Coast Guard.

Information found in this analysis was the results of hundreds of hours of meetings that all concerned were graciously willing to provide. As the results indicate, the analysis results clearly show that the Coast Guard would be better served by establishing their own AHLTA servers at the OSC center at Martinsburg, West Virginia versus connecting directly to the MTFs.

The danger of security demands changing direct connection status in the worst-case scenario, while unlikely, are a strengthening factor against direct connection to MTFs.

Table of Contents

List of Tables

Introduction

In his 2004 State of the Union address, President George W. Bush outlined his Health Information Technology Plan in which most Americans will have an electronic medical record (EMR) within 10 years. President Bush put into motion plans to use the immense purchasing power and influence of governmental health care agencies such as Medicare, Medicaid, the Community Health Centers Program, the Federal Health Benefits Program, Veterans medical care, and programs in the Department of Defense to foster the adoption of health information technology. The government has created incentives and opportunities for health care organizations to begin using EMR. The health care support industry has responded to President Bush's plan by developing a wide variety of EMR systems for health care facilities of different sizes and functions. The President's Executive order of August 22, 2006, "Executive Order: Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs" escalated the timetable and left no doubt that the EMR had to be implemented:

> By the authority vested in me as President by the Constitution and the laws of the United States, and in order to promote federally led efforts to implement more transparent and high-quality health care, it is hereby ordered as follows:
>
> As each agency implements, acquires, or upgrades health information technology systems used for the direct exchange of health information between agencies and with non-Federal entities, it shall utilize, where available, health information technology systems and products that meet recognized interoperability standards. "Interoperability" means the ability to communicate and exchange data accurately, effectively, securely, and consistently with different information technology systems, software applications, and networks in various settings, and exchange data such that clinical or operational purpose and meaning of the data are preserved and unaltered.

U. S. Coast Guard (USCG) command (CG-11) has determined due to Executive Orders that it must be running AHLTA as soon as feasible, with 2008 as the goal. Currently the USCG is utilizing the Composite Health Care System (CHCS). The purpose of this business case analysis is to determine the best structure for the integration of the AHLTA network into the Coast Guard Clinics operating systems.

Background

In order better to understand this analysis of two scenarios for connecting the Coast Guard clinics to the AHLTA network, a thorough depiction of the historical context of the current clinical information technology system used by the Coast Guard should be undertaken. The United States Coast Guard Composite Health Care System (CHCS) is a Department of Defense (DOD) developed integrated hospital information system, that provides multi-functional support to medical ancillary services in an effort to provide better patient care and accountability. CHCS supports multiple applications and outbound system interfaces to other Military Health Service systems, including the Defense Enrollment and Eligibility Reporting System (DEERS), Third Party Collection System (TPC/OHI), Laboratory Interoperability System (LIP), and Provider Graphical User Interface (P-GUI). Science Applications International Corporation (SAIC) operates and maintains the Composite Health Care System, the world's largest fully integrated clinical information system for patient information and clinical needs (SAIC, 2006). The owner of this CHCS is the U. S. Coast Guard Health Office of Health Services (CG-112), and is administered by the Health Systems and Management Division (CG-1123). Currently, the USCG maintains a network of servers in Martinsburg, WV (Foster, 2005).

The Health and Safety Directorate (CG-11) made a decision in 2002 to procure and implement the DOD's CHCS system for use by its medical clinics across the USCG enterprise.

This decision was made after CG-11 conducted the Critical Analysis and Assessment of CG CHCS, which was an evaluation of its existing medical information technology (IT) capabilities to determine the best approach to provide automated support to its medical staff in Coast Guard Clinics (Foster, 2002). The findings indicated that the current approach of utilizing CHCS as a satellite of DOD facilities did not meet the needs of timely system support, training, and file updates and it created IT problems for the Coast Guard Telecommunications & Information Systems Command (TISCOM) requiring firewall exemptions for printers across the enterprise. A typical Coast Guard clinic has a T1 connection on the Coast Guard Wide Area Network. Most clinics connected to its MTF via one of the exit points on the Coast Guard Network. These connection schemes are illustrated in figures 1 and 2 in the Appendix (Foster, 2002). Some clinics connected to its MTF over dedicated lines (56 kbps or 128 kbps), as illustrated in Figure 3 in the Appendix.

The workstation at the clinic is a PC. The Navy Internet Protocol Router Network (NIPERnet) utilized in the scheme was non-secure. Terminal emulation software was used on the PC to make a Telnet connection to the CHCS host at the MTF. In 2002, clinics were required by the DOD to discontinue Telnet due to security concerns. Additionally in some rare cases, DOD sites who hosted CG data actually billed CG for patients seen in CG facilities. Table 1 is a summary of the historical MTF host connection scheme (Foster, 2002).

Table 1

Historical Relevant Clinic Connection Schemes

Coast Guard Clinic	***Time Zone***	***Active Users (#)***	***Total Staff (#)***	***MTF***	***Connection Scheme to MTF***
Borinquen (AS)	Puerto Rico	18	18	Roosevelt Roads	T1 from Borinquen to San Juan, T1 from San Juan to Miami, T1 from Miami to Chesapeake (FINCEN) and then NIPRnet to Roosevelt Roads
San Juan	Puerto Rico	7	7	Roosevelt Roads	T1 to Miami, T1 from Miami to Chesapeake (FINCEN) and then NIPRnet to Roosevelt Roads
Baltimore Yard	Eastern	20	40	NCA	T1 to Martinsburg (OSC) and then NIPRnet to NCA
Boston	Eastern	9	30	Groton	T1 to Martinsburg (OSC) and then NIPRnet to Groton
Cape Cod	Eastern	30	30	Groton	T1 to Martinsburg (OSC) and then NIPRnet to NCA
Cape May	Eastern	69	100	NCA	T1 to Martinsburg (OSC) and then NIPRnet to NCA. Direct connect (56 kbps) to NCA
Clearwater	Eastern	18	18	Mac Dill	T1 to Miami, T1 from Miami to Chesapeake (FINCEN) and the NIPRnet to Mac Dill
CG Headquarters	Eastern	21	21	NCA	T1 to NIPRnet and then to NIPRnet to NCA
Elizabeth City	Eastern	24	25	Portsmouth	Direct connect (56 kbps) to Portsmouth
Miami	Eastern	7	16	Jacksonville	T1 to Chesapeake (OSC) and the NIPRnet to Jacksonville
Miami (AS)	Eastern	14	17	Jacksonville	T1 to Chesapeake (OSC) and the NIPRnet to Jacksonville
Portsmouth	Eastern	30	36	Portsmouth	Direct connect (56 kbps) to Portsmouth
St. Petersburg	Eastern	2	2	Mac Dill	T1 to Miami, T1 from Miami to Chesapeake (FINCEN) and the NIPRnet to Mac Dill
Yorktown	Eastern	13	26	Portsmouth	Direct connect (56 kbps) to Portsmouth
USCG Academy	Eastern	30	30	Groton	T1 to Martinsburg (OSC) and then NIPRnet to Groton
Galveston	Central	1	8	Wilford Hall	T1 to Chesapeake (FINCEN) and then NIPRnet to Wilford Hall
Houston	Central	1	8	Wilford Hall	T1 to Chesapeake (FINCEN) and then NIPRnet to Wilford Hall
Mobile	Central	12	28	Pensacola	T1 to Chesapeake (FINCEN) and then NIPRnet to Pensacola
New Orleans	Central	7	14	Keesler	T1 to Chesapeake (FINCEN) and the NIPRnet to Pensacola
Traverse City	Central	No Info	Est = 20	Great Lakes	

Alameda	Pacific	6	30	David Grant	Direct connection (128 Kbps)
Astoria	Pacific	9	12	Madigan	T1 to Seattle, T1 from Seattle to Alameda and then NIPRnet to Madigan

Table 1-*Continued*

Humboldt Bay	*Pacific*	*7*	*7*	*Madigan*	*T1 to Alameda and the direct connect (128 kbps) from Alameda to David Grant*
San Pedro	Pacific	7	7	Camp Pendleton	56 kbps direct line to Camp Pendleton
North Bend	Pacific	11	16	Madigan	T1 to Seattle, T1 from Seattle to Alameda and then NIPRnet to Madigan
Petaluma	Pacific	15	25	David Grant	T1 to Alameda and the direct connect (128 kbps) to David Grant
Port Angeles	Pacific	12	12	Madigan	T1 to Seattle, T1 from Seattle to Alameda and then NIPRnet to Madigan
Seattle	Pacific	19	23	Madigan	T1 to Alameda and then NIPRnet to Madigan
Juneau	Alaska	4	8	Elmendorf	T1 to Anchorage, T1 from Anchorage to Alameda and then NIPRnet to Elmendorf
Ketchikan	Alaska	2	11	Elmendorf	T1 to Anchorage, T1 from Anchorage to Alameda and then NIPRnet to Elmendorf
Kodiak	Alaska	15	39	Elmendorf	T1 to Anchorage (via Satellite), T1 from Anchorage to Alameda and then NIPRnet to Elmendorf
Sitka	Alaska	7	11	Elmendorf	T1 to Anchorage, T1 from Anchorage to Alameda and then NIPRnet to Elmendorf
Honolulu	Hawaii	13	24	Tripler	Direct connect (56 kbps) to Tripler. T1 to Alameda and then NIPRnet to Tripler
	Total	**460**	**719**		

Background of Current CHCS System

According to Foster (2002), the DOD initially developed and implemented CHCS in 1987. The USCG began utilizing the CHCS system in late 1993 as satellites of DOD host facilities.[1] The Coast Guard has 31 clinics in the United States and two clinics in Puerto Rico.

[1] CHCS was initially deployed in the Tidewater, Virginia area as part of the TRICARE Region 2 managed Care demonstration, and only TC Yorktown utilized CHCS and was hosted by the USN at Portsmouth.

These clinics provide health care services to active duty Coast Guard personnel as well as a limited number of dependants and retirees. Initially the Coast Guard clinics in the United States and Puerto Rico used the nearest U.S. Department of Defense (DOD) Medical Treatment Facility (MTF) for access to the Composite Health Care System (CHCS). CHCS is used primarily for patient appointments and scheduling, pharmacy, consultation, and referrals to the MTF. Most of the laboratory and radiology work is done by outside providers because many clinics are not within easy reach of the MTF. Some clinics do use the MTFs for Radiology and Laboratory services.

However, not all clinics were able to use CHCS satisfactorily. The Coast Guard command wanted to make a major commitment to CHCS as a tool for improving patient care and business process at the clinics. It was determined that a wide area network (WAN) for data, the Coast Guard Data Network (CGDN+), would be a basis for this interface (see figure 4 in the Appendix). Each Coast Guard clinic is connected to the Coast Guard WAN over a T1 line. There are four exit points on the Coast Guard WAN. These exit points connect the Coast Guard WAN to DOD NIPRnet. The exit points are in Alameda (CA), Martinsburg (WV), Chesapeake (VA), and Washington, D.C. Each exit point is protected by a firewall (Foster, 2002).

In 2002 the USCG decided to take full advantage of the CHCS capabilities by obtaining its own CHCS servers and support within the USCG enterprise.[2] An analysis undertaken then determined that changing from MTF hosts to a central network would have positive value (see table 2).

[2] Prior to CHCS, the primary CG system for collecting patient encounters and tracking medical readiness was the Clinic Automated Medical Systems (CLAMS), this was a homegrown CTOS program which was evolving slowly and sporadically into a windows based operating system

Table 2

Issues Resolved by migration to USCG Specific CHCS (Foster, 2002)

Issue: DOD MTF hosted CHCS	*Resolution: USCG specific CHCS*
Network response time slow due to NIPRnet and local MTF LAN performance issues.	All network connections now reside within CGDN+ network. USCG no longer has to compete for bandwidth over the NIPRnet.
Network sometimes unavailable and unreliable due to NIPRnet and local MTF LAN connectivity issues.	USCG has control over end-to-end connections. The CGDN+ network is less complex and more reliable than the NIPRnet.
No visibility into NIPRnet and local MTF network performance to troubleshoot issues.	TISCOM and the OSC have tools and staff dedicated to troubleshooting USCG network issues.
Print servers required due to MTF firewall configurations. Print servers are vulnerable to hacker attacks.	No need for printer connections outside of the CGDN+ network.
No single point of contact for applications or network support.	USCG now has an MIS help desk with a toll-free number as single point of contact to report all issues.
Response by MTF IS staff to support requests was slow or inadequate. No dedicated support was available for USCG issues.	Implemented a tiered support structure so all issues are logged, tracked, and responded to within 3 business hours. On-site DBAs at Alameda, CA and Portsmouth, VA provide immediate support to MLCs.
File/table builds were not standardized for all Coast Guard clinics.	All file/table builds are customized for USCG and standardized for all clinics.
Training was not standardized or specific to USCG clinic operations	Training is specific to USCG needs. Customized curriculum, on-site and web-based training, and tracking of clinic staff training records are provided.

Table 2-*Continued*

Custom reports for USCG management purposes not available.	On-site DBAs provide reports for MLC and HQ management.
No single point of contact for applications or network support.	USCG now has an MIS help desk with a toll-free number as single point of contact to report all issues.
Response by MTF IS staff to support requests was slow or inadequate. No dedicated support was available for USCG issues.	Implemented a tiered support structure so all issues are logged, tracked, and responded to within 3 business hours. On-site DBAs at Alameda, CA and Portsmouth, VA provide immediate support to MLCs.

The USCG in November 2002 implemented the DOD CHCS at the Operational Service Center (OSC) in Martinsburg, WV (Foster, 2005). CHCS provides all USCG medical clinics with automation support to its medical and ancillary staff. The USCG users access CHCS from within the Coast Guard Data Network (CGDN+) from their Standard Workstation III (SW III) desktop, while the servers are located within a firewall protected safe zone at the OSC. The protected zone, hosted at OSC Martinsburg, serves as an entry point to the USCG application servers. The protected zone provides a secure location to host the CHCS servers, provides a secure connection to the commercial Internet, and segregates outside external business partners from the CGDN+ network. All traffic going to the USCG OSC is encrypted using the standard SSL port 443. The USCG CHCS components residing at the OSC are located behind OSC established firewalls.

Concept of Operation

The Coast Guard CHCS platform consists of nine HP/Compaq AlphaServer DS10 systems according to Foster (2005). The architecture of CHCS was designed for one server at each MTF; thus, there is no provision for multiple time zones within each server. This architecture is continued in AHLTA. The time zones for Alaska (AK), Central (CEN), Hawaii (HI), and Puerto Rico (PR) each uses one HP/Compaq AlphaServer DS10 system with 512MB memory and Fiber Channel based disk subsystem (total 4 systems). The Eastern (EAST) time zone uses three HP/Compaq AlphaServer DS10 systems with 1GB memory each. The Pacific (PAC) time zone uses two HP/Compaq AlphaServer DS10 systems with 1GB memory each. Because the EAST and PAC systems are in OpenVMS cluster configuration, they have built-in redundancy and failover in the event one of the systems fails. The remaining time zone systems are single node and do not have automatic redundancy and failover. The redundancy and failover for the AK, CEN, HI, and PR systems are provided by a hot standby system, which can be brought on-line to replace a failed system using remote system management.

Foster (2005) continues that the data storage subsystem is an HP/StorageWorks disk subsystem with dual redundant Fiber Channel Switches (HSG80). All systems have dual Fiber Channel connections to the HP/StorageWorks disk subsystem. Data isolation between systems will be provided by a StorageWorks technique called connection enabling. Each time zone system or systems and its respective data volumes have its connection enabled while the other systems have their connections to the data volumes that do not belong to them disabled. This technique will provide access to data volumes that belong to the system and prevent other systems from accessing the data volumes. In an effort to reduce cost, OSC Martinsburg is not required to provide operators for attended backup tape operation.

The Coast Guard users are connected to the CHCS platform over the CGDN+. This connection is provided by a standard Telnet protocol using the TISCOM-approved Citrix client software product found standard on the Workstation III. A local system management console is used to perform system management tasks when physical presence is required at the OSC. All remote tasks, such as troubleshooting, system management, and user support are performed via the Internet, CGDN+, and the Non Internet Protocol Router Network (NIPRNET). The platform contains a ConsoleWorks Server (CWS) that allows access to consoles of systems and other devices for the purpose of remote systems management at the OSC (Foster, 2005). The Coast Guard is dedicated to the Citrix solution, and new thin terminals have been installed in all clinics offices and are being installed in all clinic treatment rooms (T. J. Kulzer, personal communication, March, 2007). The ability to remotely manage terminals is highly advantageous in the Coast Guard situation of small clinics in isolated locations.

All communication from Remote Support Sites (non-Coast Guard locations) to OSC is over encrypted links utilizing Secure Socket Layer (SSL) for browser connections. All communications from Coast Guard clinics over the CGDN+ to OSC use the existing links to CGDN+. All the existing links between Coast Guard clinics and OSC are behind the Coast Guard firewall.

In August 2002, the CG-112 awarded a competitive contract to Science Application International Corporation (SAIC) and Federal Technology Corporation (FEDTEC) for implementation, training, engineering, and continuation support of the USCG CHCS. The system was deployed beginning in November of 2002 and is sustained under the above referenced contract (Foster, 2005).

The USCG CHCS system collects and maintains Sensitive but Unclassified personal health information (PHI) on all USCG active duty members, dependents, retirees and their dependents being treated in a USCG medical clinic. The protection and release of this data is carefully controlled by the system. There are various methods for providing protection both while collecting the information and during the course of patient care. Foster (2005) addresses the system level controls to maintain security of the data while at rest in the system.

The user level controls are authorized by security keys, which are assigned by the local System Administrator (SA) at the clinic level, based on the role the user plays in the treatment of the patient. Security keys function like door locks and door keys, locking and unlocking menu options for CHCS users. Any menu option may have a security key associated with it. Once a security key is assigned to an option, only users with the same security key may access that option. This means that any menu tree can be selectively restricted at any point.

These keys are defined at appropriate functionality levels. For example, a front desk clerk has certain keys that limit that individual's access to collection and release of data. Should a user require access to more than one functionality, multiple keys may be assigned to that individual based on the roles that individual plays in his or her use of the system. The system has the capability to audit at the functionality level the keystroke actions that that individual performed. The release of patient data by an individual is limited to the assigned role of that individual. A check-in clerk without pharmacy privileges cannot order a prescription or issue medications from the system. This role-based security is managed locally by the SA. The users at each facility are limited to the type and class of data to which they have access.

The CHCS database, which contains "files and tables" (which are unique to the USCG medical and are required to support such actions as establishing a pharmacy formulary, appointment types, and other USCG medical files) along with patient information, is accessible by only trusted contractor Database Administrators (DBA). The user can only access that data which is necessary to provide patient care as designated by the local SA (Foster, 2005). Since these files and tables are now unique to the Coast Guard, combining the system back to satellite clinics off MTFs would entail massive recoding.

The system is located in Martinsburg, West Virginia at the OSC, and allows users to connect over the CGDN+ network. The only significant change from the DOD model is the centralized hosting location at the OSC and the deliberate use of the CGDN+ network as the backbone for user access. No user can access the system remotely unless given specific authorization. The system resides in a safe zone, where only access to the CGDN+ network is available. The OSC maintains control of our access and periodically monitors the pathway. The only external connection to CHCS (from outside CGDN+) is provided via a Virtual Private Network (VPN) through the MHS domain managed by Defense Information Systems Agency (DISA) and then only to authorized receivers and senders of data. These interface partners have been designated by DISA and USCG staff as trusted agents. Most either are DOD entities or entities under contract such as the commercial laboratories, DEERS, MHS systems, and USCG Tiered support. All PHI data being transmitted through the VPN is encrypted (Foster, 2005).

The initial implementation of CHCS completed May 2003 provided on-site training for all users and designated System Administrators. The ability to provide remote Tiered support and system management actions is intended to limit impact on the staff at medical clinics.

CHCS is the only comprehensive medical information system currently available to the USCG clinical staff. The implementation of CHCS afforded the clinical staff an excellent opportunity to concentrate strictly on patient care and let the by-products of medical automation provide the outputs necessary for upward reporting. Prior to the implementation of CHCS no system existed that would capture patient encounters and store that information centrally. The CHCS architecture is modeled in figure 5 in the Appendix.

User Impact

Each CHCS USCG user is assigned specific roles and responsibilities based on the application or clinical module they require in performance of their medical duties. Example: The appointing clerk would have no user-based role to access a patient's medication file unless given those privileges by the clinic system administrator. The assignment of system privileges is the responsibility of local system administrators based on the medical role of the user.

Environment

The OSC at Martinsburg provides physical and network security that ensures adequate protection of the PHI data. TISCOM has identified CHCS as a potential risk to CGDN+ with its connection to external business partners such as DEERS, Internet and NIPRNET connections, and as such has limited CHCS to a protected environment within the OSC and a segregated network connection from the CGDN+. OSC has established a firewall between the CGDN+ and CHCS. These measures, coupled with the CHCS system level security features, pending DITSCAP certification, Virtual Private Network (VPN) managed by the Defense Information Systems Agency (DISA) and CG assignment of static IPs for Tiered Support, provide a more than reasonable level of trust (Foster, 2002).

Operational System Environment

The USCG CHCS at the OSC in Martinsburg, WV meets the DOD Information Assurance (IA) IT Requirements. Implementation of this level of security helps ensure that appropriate controls are in place to protect the privacy of patient data in accordance with federal laws. Additional detailed security requirements are defined and approved through the DITSCAP. CHCS in DOD was DITSCAP certified and accredited 11 January 2003 with the following constraints (Foster, 2002):

- CHCS has no environmental concerns other than those required for normal computer room operations. The OSC at Martinsburg has met all environmental requirements.
- CHCS will follow the approved firewall exemption process. All firewall exemptions obtained to date have been approved by TISCOM.
- The external business partners are connected to the USCG CHCS system through a VPN domain managed by DISA.
- Tiered support is provided by controlled access using Static IP/SSL
- To access the CHCS system from inside CGDN or outside either in the protected zone or from external interfaces password controls are in place.

Operational User Environment

Each site is required to provide physical security protections to ensure only authorized users have access to system resources. Common access control policies[3] are instituted to control physical access as well as online user access to CHCS resources and applications. These are (Foster, 2002):

- USCG WS III Hummingbird Terminal Emulations Software is used to access CHCS.
- The protocol used by Hummingbird is Telnet. There is no PHI data stored on the WS III's.
- CGDN+ is the network used by USCG system users and is deemed to be a Trusted Network.
- Workstation III is the desktop used by USCG CHCS users.

[3] Common access control policies refers to the host site-implemented access control set of procedures that are driven by basic guidance provided by the MHS Security Policy and CHCS Security Policy.

- Non-standard Workstation is employed to support limited applications and prior approval is requested by TISCOM through the Engineering Change Proposal process before implementing.

Operational External User Environment

Defense Enrollment Eligibility System (DEERS) is the system of record for documenting eligibility for medical and other benefits for service members and dependents. It is a familiar interface for all service members. The quality and timeliness of service are determinants of morale. The Director of Information Management initiated this project to identify improvements in timeliness and quality of service. The recommended improvements have strengthened the management of data and decreased the time required for a correct update cycle, providing better service to each customer. There are approximately 104 MTFs where USCG shares medical information such as pharmacy and medical consulting (Foster, 2002).

AHLTA

AHLTA is the enterprise-wide electronic health records system for the Department of Defense (DOD) Military Health System (MHS). The AMEDD has now deployed the outpatient component (Block 1) to all MTFs. AHLTA leverages advanced technology to its fullest potential, ensuring healthcare providers have instant access to invaluable medical information about their patients. According to the Clinical Information Technology Program Office (CITPO, 2006), AHLTA equally as capable in field mobile units as it is in peacetime medical centers. AHLTA is described by CITPO as:

- Powerful - Valuable, life-saving beneficiary information is available 24/7.

- Legible - Beneficiary records are complete, accurate and clear.

- Secure - Only authorized users can access records and they are protected from natural or fabricated disasters.
- Longitudinal - Data migration from CHCS is being performed by pulling 25 months of laboratory, anatomic pathology, pharmacy, and radiology data to populate the Clinical Data Repository (CDR). The CDR is a central database of individual, electronic, lifetime patient records that users can access, analyze, and add to, right at the point of care. Consolidating MHS data within the CDR reduces risk, saves time, and improves clinical decisions by providing efficient, centralized access to a patient's lifetime medical record at the point of care. Data migration preserves the investment in existing legacy information systems by easily exchanging data through open system architecture and standards compliance, according to conversations with H. Moos, RITPO in October, 2006.
- Knowledgeable - Offers healthcare providers wellness reminders for their patients.
- Efficient - Interoperability ensures that costly tests, labs and scans are not needlessly duplicated.
- Proactive - AHLTA provides critical information that lets healthcare providers know about disease outbreaks, allowing early intervention in targeted populations.

This medical surveillance facilitates military force health protection.

Since full-rate deployment started in January 2004, fielding and use of AHLTA has experienced many challenges. Various issues delayed the fielding of the local cache (failover mode) Build 838, but it is now being deployed. The Executive Order "Executive Order: Promoting Quality and Efficient Health Care in Federal Government" has determined that the

Coast Guard will transition to AHLTA. As the pGUI interface of our CHCS system will no longer be supported by the DOD, the transition to AHLTA should be done with all due speed. The architecture of AHLTA utilized by the DOD is summarized by figure 6 in the Appendix (Ray, 2006).

Note that the Legacy CHCS servers, surrounded by the Caché including objects, and the local cache server are collocated at the MTF. Thus, all the local clinical workstations are within the firewall. The Coast Guard would modify this design in that all systems would be co-located at the USCG Operations Systems Center (OSC), Martinsburg, WV (see figure 7 in the Appendix).

The Coast Guard is therefore burdened with needing to maintain a secure, high quality wide area network (CGDN+). Capacity planning must entail the ability to adequately support, 32 clinics across the U.S. and Puerto Rico, 250,000 encounters per year across USCG enterprise, 250 providers (780 total users), and 114,000 patients across all time zones.

Before undertaking data migrations from legacy systems, CITPO data analysts go through a two-step process of data profiling and data mapping. First data profiling is a review of the source data to understand its content, structure, quality and integrity. Once data has been profiled, a set of mapping specifications is developed based on this profile. That is the process called data mapping. When done with the necessary exacting precision, data profiling and mapping lower project risk and deliver higher data quality according to H. Moos, RITPO in October 2006. The process of data mapping becomes programmatic when data from Coast Guard clinics is mingled with MTF data, since each entity may have different mapping requirements.

The Resource Information Technology Program Office (RITPO) has performed extensive testing for the configuration of the AHLTA servers. In the business case analysis entitled

"Independent Business Case Analysis of the Military Health System Enterprise Blade Server Technology Refresh Initiative for the Resources Information Technology Program Office" (2006), it was determined that utilizing Egenera Blades and BladeFrames as servers was the most cost effective configuration despite higher initial cost due to decreased support, power, and cooling demands. The advantage increases if their increase power allows other servers to be replaced. The Coast Guard therefore might consider a system designed around blade servers although the lower demands of the Coast Guard may prove this not advantageous.

Methods and Assumptions

Scenario and Data

Through analysis with CG-1123, it has been determined that there are two courses of action:

1. The Coast Guard can negotiate to reestablish direct linkages with MTFs
2. The Coast Guard can obtain and maintain servers in OSC currently in Martinsburg.

Scope

This period will be through FY 2012, the normal Coast Guard period for IT development. This analysis must also determine the choice that will position the Coast Guard in a favorable position for possible missions to be determined by Homeland Security. The geographical scope is that of the entire Coast Guard organization served by medical services, including those referred to DOD facilities.

Financial metrics

The Business Case Analysis (BCA) will use an economic model that was developed to meet the requirements of the OMB's Circular A-94: *Guidelines and discount rates for benefit-cost analysis of federal programs* (OMB, 2007). The BCA model will utilize the Discount Rate given in “Appendix C: Discount Rates for Cost-Effectiveness, Lease-Purchase, and Related Analyses for OMB Circular Number A-94” (OMB, 2007). The rate given for the 5-year maturity in the table “Real Interest Rates on Treasury Notes and Bonds of Specified Maturities” is 2.6%. The endogenous variable for the financial evaluation of the two scenarios is net present value (NPV). This case will use a differential model of analysis, since many of the costs will be identical for both scenarios, and may not be available for this document. Examples of these costs are CDR/AHLTA cost share and AHLTA training costs.

Business Impacts

Benefits

The benefit that is critical to the case is the availability of high quality AHLTA performance that will be readily accepted by the clinicians while satisfying the Executive directive for an electronic health record. Connection directly to MTFs gives the advantage of fewer systems for the Coast Guard to manage. Further benefit to be valued is flexibility associated the control of the system. These values will be valued in accordance with guidelines obtainable in the Coast Guard Health and Safety Directorate (CG-11).

Costs

This BCA will concentrate on the true cost of making AHLTA available to healthcare personnel at a performance level that is satisfactory for success of the operation. Financial metrics will be scenario contingent. Metrics to be measured include costs of obtaining and operation of servers, costs of maintaining the different networks needed by the different scenarios to include negotiated costs with MTFs, costs associated with loss of availability AHLTA. These will be determined by querying Coast Guard network specialists, operational elements of TRICARE Management Activity, and government contractors involved in current and historical systems.

Acquiring AHLTA by direct connection to MTF environment will be considered first.

- Historically the Coast Guard has developed Memorandam of Agreement (MOA) with each individual MTF that provided direct connection and IT services necessary to maintain this connection. Some of these agreements were altruistic on the part of the services, while other agreements treated the Coast Guard as a revenue source. These ranged from no charge to $500,000/year (R. R. Miller, USCG CG-11, personal communication, 2007). New MOA for each MTF would have to be negotiated. It is expected with the tighter fiscal control in the MTF environment, a cost of $1,000,000 is estimated by SAIC and verified by the CG-1123 IT specialist (D. Fielden & T. J. Kulzer, personal communication, February 2007)
- New workstations for each FTE user must be anticipated. Due to security requirements of TISCOM, none of the thin client workstations currently in use could be connected to both the CGDN+ and to the DOD AHTA environment concurrently. Thus, an estimated 800 (range 700-900) workstations running Windows software at a cost of $25000 would need to be purchased for a total cost of $2,000,000 per SAIC and verified by the CG-1123 IT specialist (D. Fielden & T. J. Kulzer, personal communication, February 2007).
- These computers and printers would also have need for on-site Windows and software administrative support, as they could not be thin clients with Hummingbird control. This is estimated to cost $70,000 annually by SAIC and verified by the CG-1123 IT specialist (D. Fielden & T. J. Kulzer, personal communication, February 2007).

- New printers to be connected to the DOD-Windows environment would be necessary with an estimated additional cost of $375,000 (G. Jewell, personal communication, March 2007).
- An additional infrastructure for this network would need to be put in place estimated at $100,000 per clinic average for a total of $3,300,000 (T. J. Kulzer, personal communication, February 2007)
- Since the CG and DOD use different data storage models, there would be incurred a cost of data conversion, estimated by CITPO to be $25,000 (J. Lopata, personal communication, January 2007).

Non-financial, but very serious costs to be considered of this scenario are those caused by loss of autonomy for the Cost Guard. Changes in security for the MTF IT commands, and MTF commanders' interpretation of proper security could cause unexpected and unacceptable losses of AHLTA. In executive information decision systems such as M2, the CG productivity statistics would show up as a satellite of the MTF, making management of the CG clinic difficult. These costs are summarized in table 3.

Table 3

Costs Associated with Direct Connection to MTFs

Year	2008	2009	2010	2011	2012	2013	Totals
Workstations	2,000,000	0	0	0	0	0	2,000,000
Printers	375,000	0	0	0	0	0	375,000
Direct MOA	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000	6,000,000
Data conversion	25,000	0	0	0	0	0	25,000
Workstation support	50,000	50,000	50,000	50,000	50,000	50,000	300,000
Total	3,450,000	1,050,000	1,050,000	1,050,000	1,050,000	1,050,000	8,700,000

Next, we consider the alternative, purchasing and utilizing AHLTA servers, one for each time zone, at OSC in Martinsburg, WV.

- Planning for the more versatile Engenera blade servers, a cost estimate of $269,000 plus $100,000 for the EMC Clarion disk subsystem gives a total cost of $369,000 with annual upgrades at $20,000 (V. K. Dutto, personal communication, September 2006).
- Using national averages, *Computer Economics* ("Benchmarking Costs per Server Instance", 2007) reports an annual cost of $20,700 each for Windows servers. Support for the six servers therefore is computed at $124,200 per annum.
- According to G. Jewell (personal communication, March 2007), discussions with Tri-Service Infrastructure Management Program Office (TIMPO) indicate that they would want to implement circuits to both Montgomery and the backup San Antonio Defense Enterprise Computing Center Detachment (DECC). The estimate from TIMPO was the Coast Guard would need around 2Mbps. This could be done with a partial-T3 (4.5Mbps) or just two T1's (1.44Mbps each). The costs from DISA are summarized in

table 4. Utilizing two T1 lines appears to be the better solution.

Table 4

Costs Associated with Connection of Servers to the CDR (Jewell,2007)

	Cost per Circuit		Circuits	Cost all circuits		Yearly costs	
	1-time	Monthly	Needed	1-time	Monthly	1st yr	Out years
Martinsville, WV - San Antonio, TX							
T-1	1,000.00	920.11	2	2,000.00	1,840.22	24,082.64	22,082.64
4.5MB	1,000.00	6,645.99	1	1,000.00	6,645.99	80,751.88	79,751.88
Martinsville, WV – Montgomery AL							
T-1	2,000.00	1,562.00	2	4,000.00	3,124.00	41,488.00	37,488.00
4.5MB	5,000.00	6,075.00	1	5,000.00	6,075.00	77,900.00	72,900.00
					2-T1	65,570.64	59,570.64
					4.5MB	158,651.88	152,651.88

- There will also be a cost associated with continued compliance with the requirements of the Coast Guard Data Network. These will total approximately $12,000 per year (T. J. Kulzer, personal communication, February 2007).

Table 5 contains the summation of costs associated with Coast Guard AHLTA from the above calculations.

Table 5

Costs Associated with Coast Guard AHLTA Servers

Year	2008	2009	2010	2011	2012	2013	Totals
Servers	369,000	20,000	20,000	20,000	20,000	20,000	469,000
Server support	124,200	124,200	124,200	124,200	124,200	124,200	745,200
Connection to CDR	65,791	59,971	59,971	59,971	59,971	59,971	365,646
CGDN+ compliance	12,000	12,000	12,000	12,000	12,000	12,000	72,000
	570,991	216,171	216,171	216,171	216,171	216,171	1,651,846

Utilizing the government disount rate of 2.6%, a Net Present Value (cost) for conection to MTFs is ($8,177,408.38). A similar calculation for the scenario of Coast Guard AHLTA servers gives a NPV of ($1,544,256.33). This results in a differential cost-savings advantage of $6,633,152.05 for developing Coast Guard AHLTA servers in Martinsburg.

Major assumptions

1. AHLTA must be implemeted.
2. AHLTA will have the requirement that servers separate from legacy CHCS servers be utilized.
3. The Coast Guard Data Network will be made available by TISCOM for Citrix AHLTA placement and be robust enough to transmit AHLTA.
4. TISCOM will require the DOD network and CGDN+ network be phiscally separated.

Sensitivities, Risks, and Contingencies

The key factor is the sensitivity of the project to the costs of maintaining connectivity to AHLTA. Factors to be measured include negotiated memorandam of agreement for connection and cost of systems maintenance for both scenarios. Contingencies that may affect the studies include changes in control of MTFs caused by the Medical Joint Cross-Service Group (JCSG), which reviewed Department of Defense healthcare functions and provided base closure and realignment (BRAC) recommendations and changes in force management. A unified DOD command may be able to better make a single MOA of connection, rather than the current situation where each MTF commander is able to negotiate his/her own agreement and requirements. If the MTF MOA for connection was offered for free, this would make this choice more competitive, but still more costly at NPV of ($2,675,114.68). This is judged very unlikely by R. R. Miller, CG-11 in a personal conversation in February 2007. If a direct connection to the MTFs were undertaken, a change in policy of the commander leading to a loss of connectivity could result in the Coast Guard scrambling to reestablish connectivity to the CDR through developing their own servers in an emergency arrangement. This would be the worst case scenario, with the cost exceeding the two scenarios combined ($9,721,665) due to the inefficiencies of waste as determined by this author. The major driver of the cost differential is the requirement that the DOD network and the CGDN+ remain physically separated. If this were to change, a reanalysis would be in order.

Recommendations and Conclusions

The purpose of this analysis was to determine the direction for the establishment of AHLTA and connection to the CDR by the Coast Guard. U. S. Coast Guard (USCG) command (CG-11) has determined due to Executive Orders that it must be running AHLTA as soon as feasible, with 2008 as the goal. Currently the USCG is utilizing the Composite Health Care System (CHCS). Two scenarios are investigated in this analysis: The Coast Guard must therefore deliver AHLTA to its clinics, either through direct connection to military treatment facilities (MTFs), making the clinics satellite clinics, or through developing their own servers at the Operational Service Center (OSC) complex in Martinsburg.

As a result of this study, as well as much work by the Coast Guard Health Systems

Management Division (CG-1123), the DOD is strongly considering implementing a pilot study to help fund the Coast Guard server networks. As describe earlier, the plan to connect clinics to the OSC uses thin clients at the clinics with Citrix solution management pushing programs down from Martinsburg. The DOD is interested in that deployment structure for future generations of AHLTA. Having the ability to centrally upgrade and monitor the programs, instead of having to send technicians to the site is viewed as a strong advantage. While this is more critical in the Coast Guard with our small, isolated clinics, the DOD is still very interested in cost savings of this arrangement.

This analysis looked at as many factors as possible affecting the scenarios. Experts in their field in the DOD, military, contractor and government service, contractors, and Coast Guard Directorates CG1 and CG6 were all queried. Information found in this analysis was the results of hundreds of hours of meetings that all concerned were graciously willing to provide. As the results indicate, the analysis results clearly show that the Coast Guard would be better served by establishing their own AHLTA servers at the OSC center at Martinsburg, West Virginia versus connecting directly to the MTFs. The danger of security demands changing direct connection status in the worst-case scenario, while unlikely, are a strengthening factor against direct connection to MTFs.

The electronic health record will become the standard of care in the near future. According to this analysis, the Coast Guard will be better served by establishing its own network of servers to deliver AHLTA, rather than relying on the DOD MTFs to deliver AHLTA.

References

Benchmarking costs per server instance. (2007, February). *Computer Economics.* Retrieved 24 February from http://www.computereconomics.com/custom.cfm?name= 1199

Bush, G. W. (2006, August). *Executive order: Promoting quality and efficient health care in federal government administered or sponsored health care programs.* Retrieved 14 September 2006 from http://www.whitehouse.gov/news/releases/2006/08/print/20060822-2.html.

Clinical Information Technology Program Office. (2006). *CITPO home page.* Retrieved 15 September, 2006, from http://www.tricare.osd.mil/peo/citpo/default.htm

Foster, M. (2002, April). *Critical analysis and assessment of Composite Health Care System (CHCS) capability at United States Coast Guard (USCG) clinics*, available from Science Applications International Corporation (SAIC), Enterprise & Health Solutions Sector (E&HSS), 5107 Leesburg Pike; Suite 2200, Falls Church, VA

Foster, M. (2005, November). *Automated Information System (AIS) document for the Composite Health Care System (CHCS).* Availible from United States Coast Guard Headquarters, 2100 2nd Street, SW, Washington, D.C. 20593-0002

Independent business case analysis of the military health system enterprise blade server technology refresh initiative for the Resources Information Technology Program Office. (2006, February). Available from Resources Information Technology Program Office, 5205 Leesburg Pike, Skyline 1, Suite 1100, Falls Church, VA 22041-3206

Office of Management and Budget. (2007). *OMB circulars.* Retrieved 15 February, 2007, from http://www.whitehouse.gov/omb/circulars/a094/a94_appx-c.html

Ray, L. (2006, Summer). *AHLTA data flow.* unpublished document.

Resources Information Technology Program Office. (2006). *RITPO home page*. Retrieved 15 September, 2006, from http://www.tricare.osd.mil/peo/citpo/default.htm.

Appendix

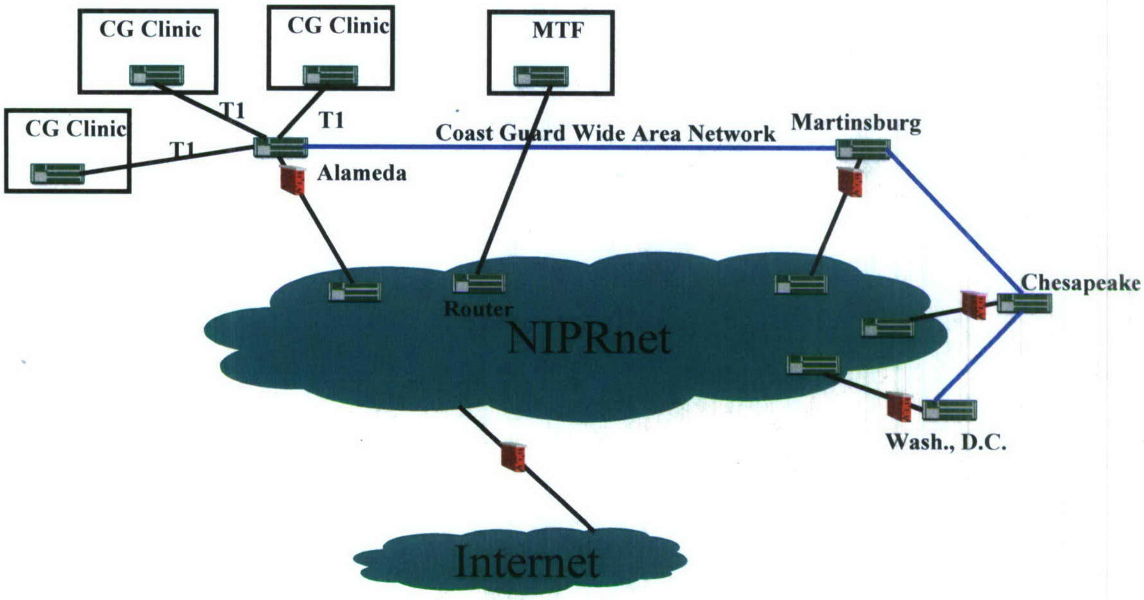


Figure 1. Clinics LAN to Coast Guard WAN Connection Scheme

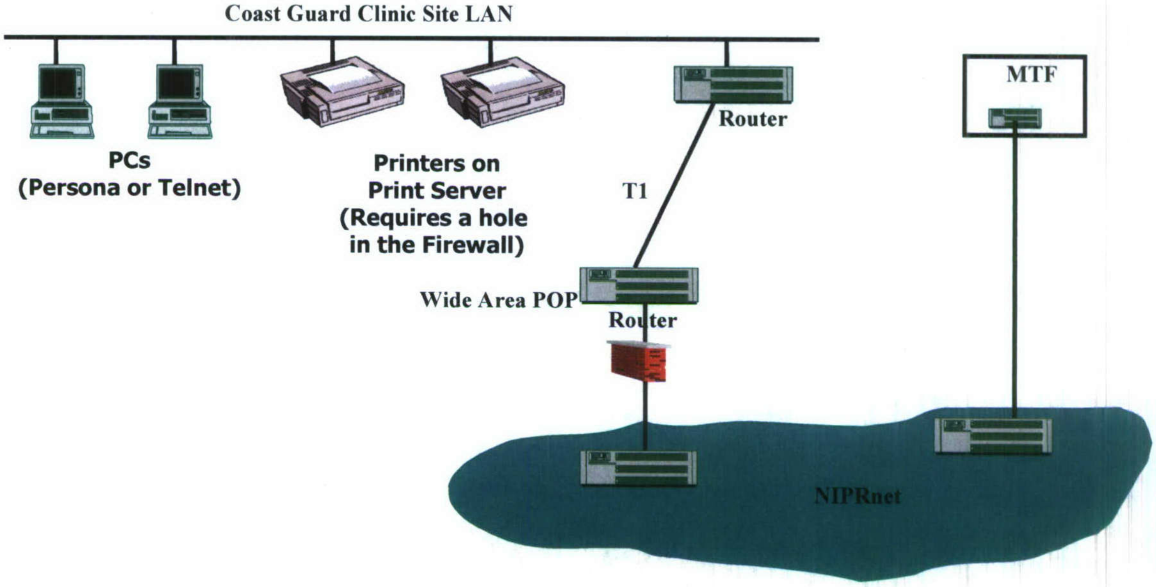


Figure 2. Clinic LAN to MTF Connection Scheme via NIPRnet

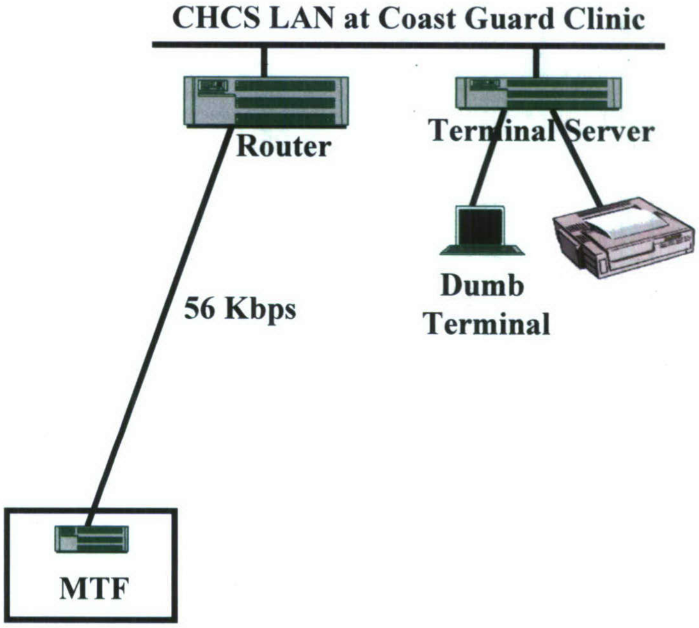


Figure 3. Clinic to MTF Direct Connect Scheme

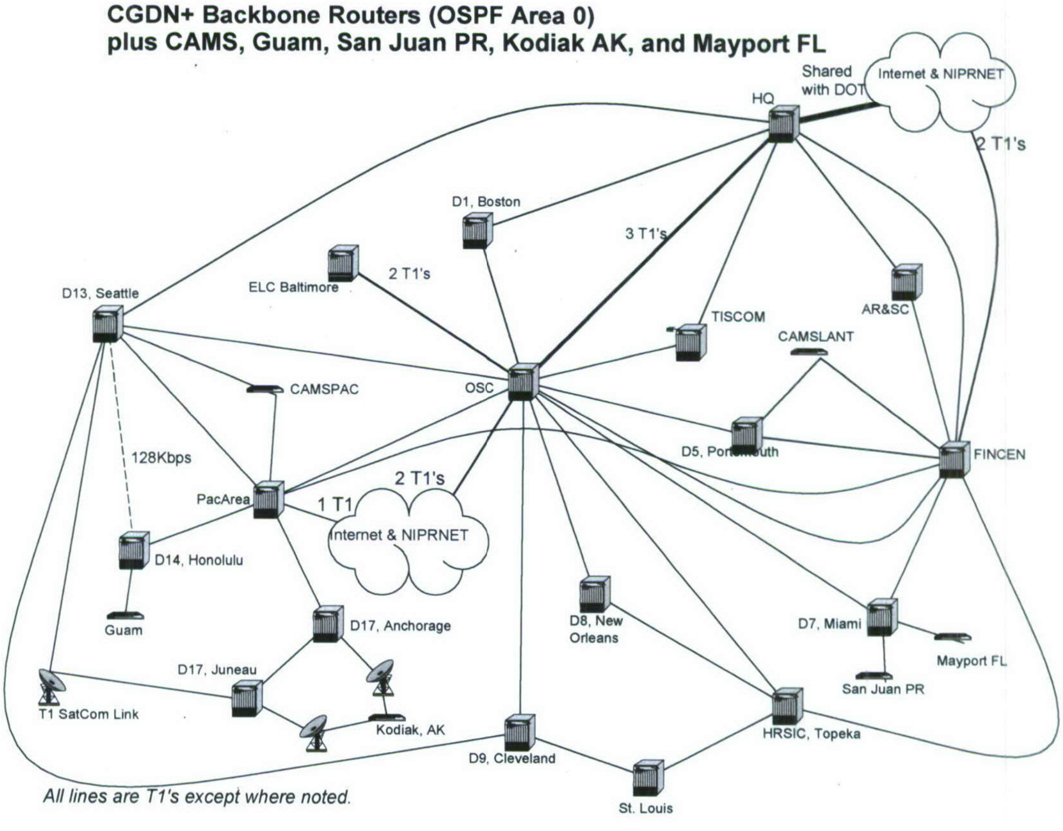


Figure 4. Coast Guard Wide Area Network

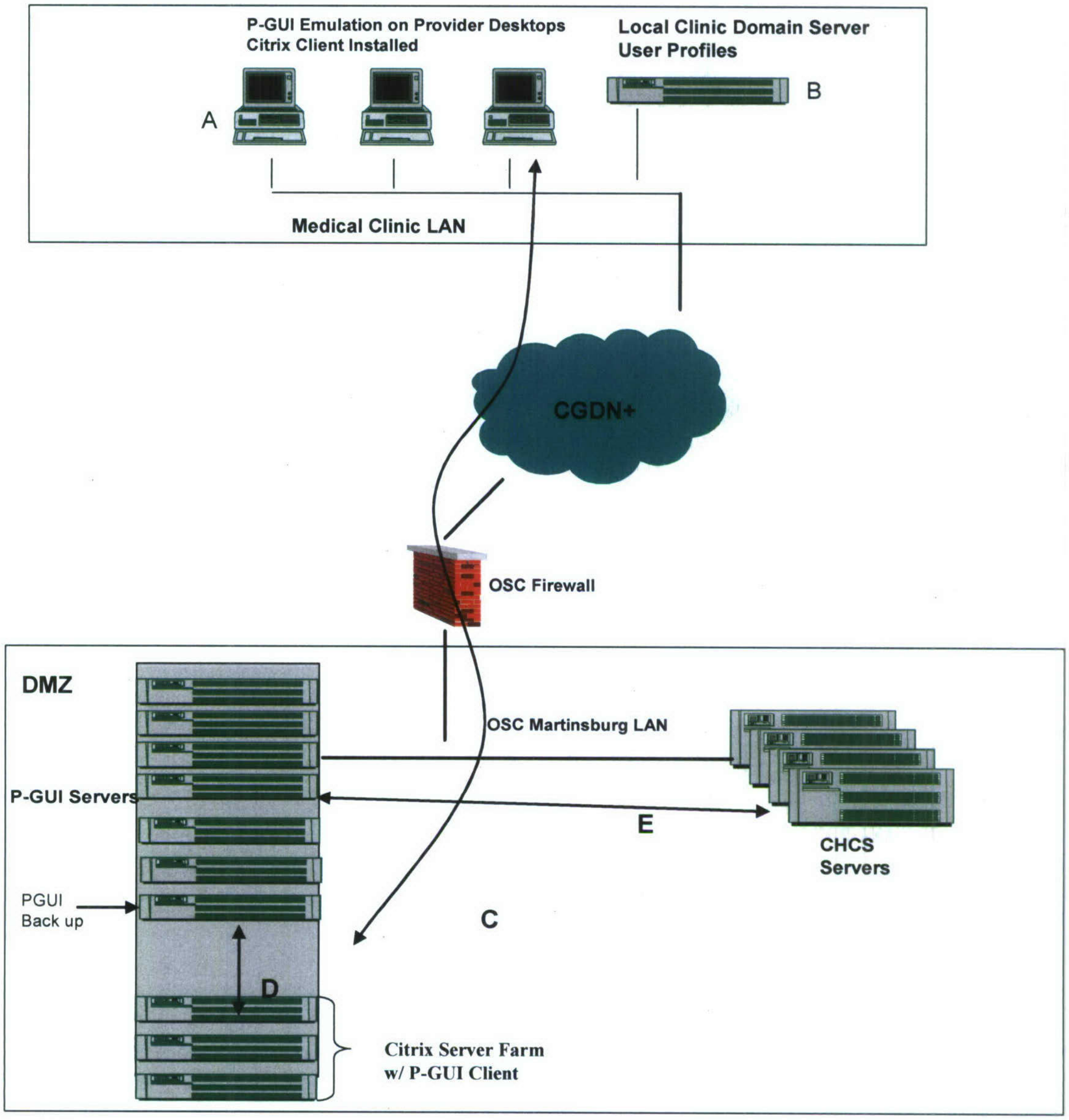
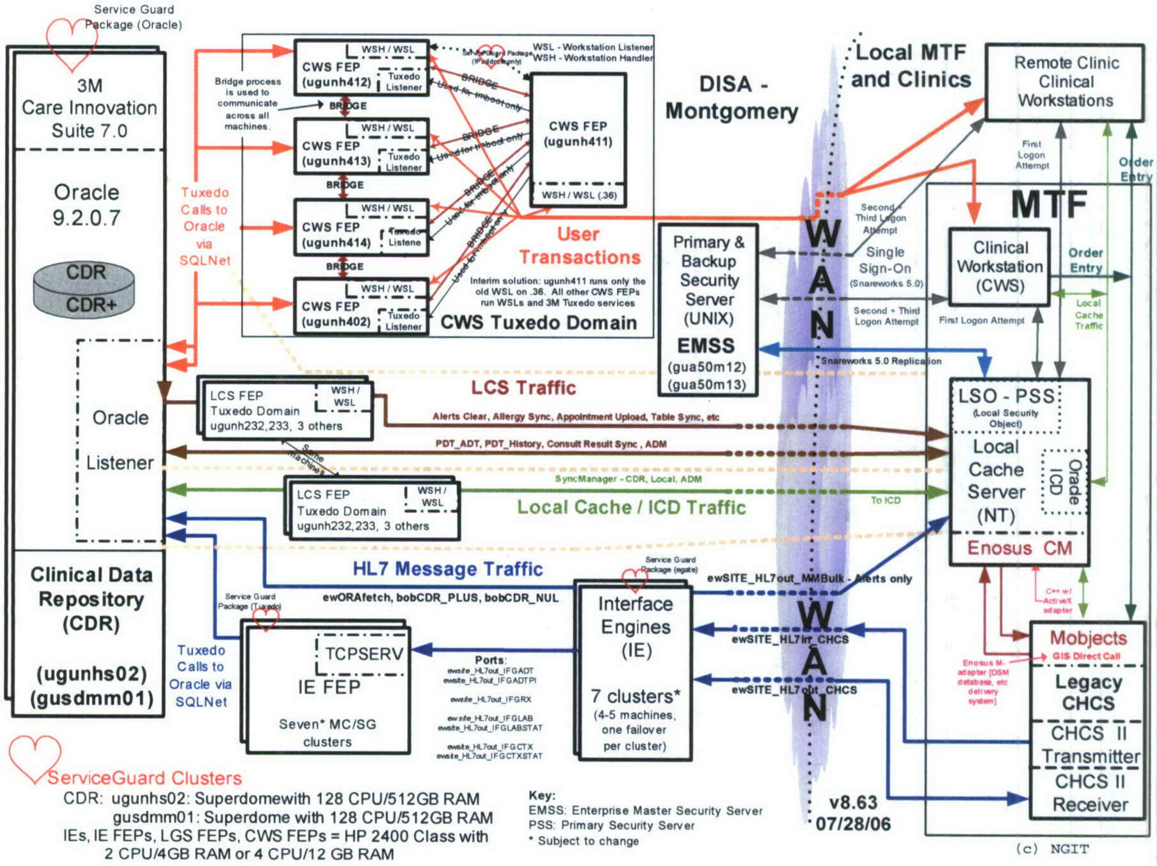


Figure 5. The USCG CHCS architecture (Foster, 2005).

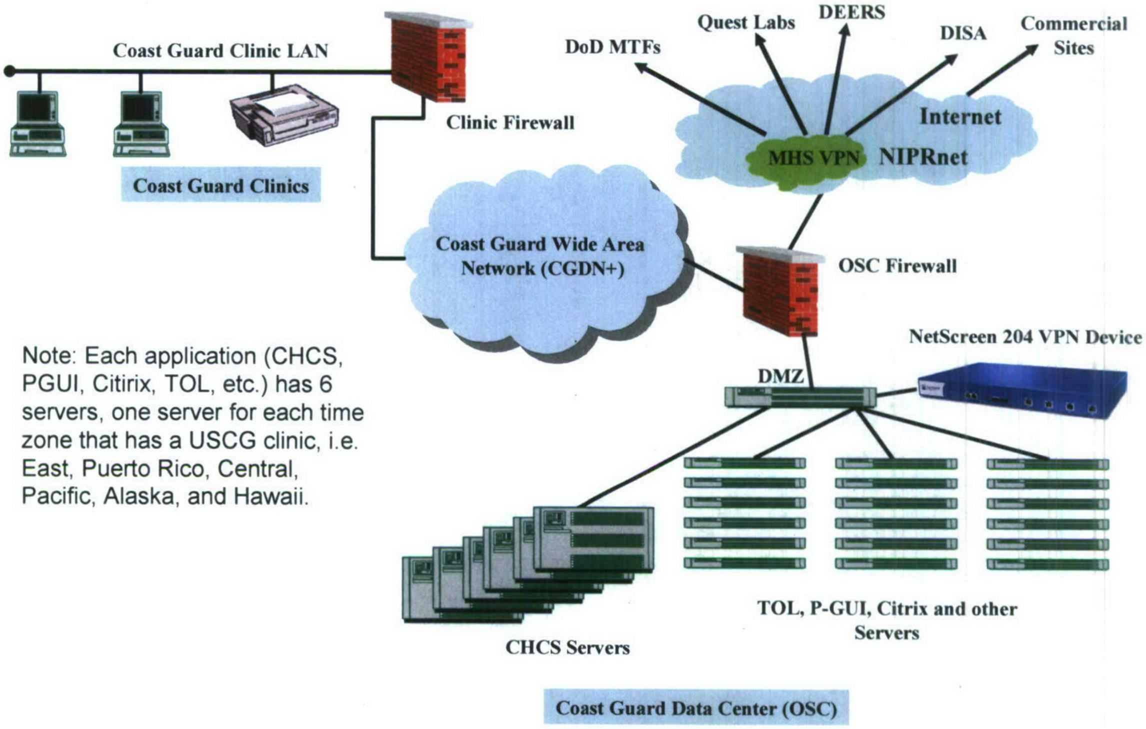
Note. Each system/cluster is a separate entity with its own database


Service Guard Package (Oracle)
3M Care Innovation Suite 7.0
Oracle 9.2.0.7
CDR
CDR+
Oracle Listener
Clinical Data Repository (CDR)
(ugunhs02)
(gusdmm01)
Tuxedo Calls to Oracle via SQLNet
Bridge process is used to communicate across all machines.
BRIDGE
CWS FEP (ugunh412)
CWS FEP (ugunh413)
CWS FEP (ugunh414)
CWS FEP (ugunh402)
WSH / WSL
Tuxedo Listener
Service Guard Package (IP address only)
WSL - Workstation Listener
WSH - Workstation Handler
BRIDGE
Used for imboot only
CWS FEP (ugunh411)
WSH / WSL (.36)
User Transactions
Interim solution: ugunh411 runs only the old WSL on .36. All other CWS FEPs run WSLs and 3M Tuxedo services
CWS Tuxedo Domain
DISA - Montgomery
Primary & Backup Security Server (UNIX)
EMSS
(gua50m12)
(gua50m13)
LCS FEP Tuxedo Domain ugunh232,233, 3 others
WSH / WSL
LCS Traffic
Alerts Clear, Allergy Sync, Appointment Upload, Table Sync, etc
PDT_ADT, PDT_History, Consult Result Sync , ADM
Same machines
SyncManager - CDR, Local, ADM
Local Cache / ICD Traffic
To ICD
HL7 Message Traffic
ewORAfetch, bobCDR_PLUS, bobCDR_NUL
Service Guard Package (Tuxedo)
Tuxedo Calls to Oracle via SQLNet
TCPSERV
IE FEP
Seven* MC/SG clusters
Ports:
ewsite_HL7out_IFGADT
ewsite_HL7out_IFGADTPI
ewsite_HL7out_IFGRX
ewsite_HL7out_IFGLAB
ewsite_HL7out_IFGLABSTAT
ewsite_HL7out_IFGCTX
ewsite_HL7out_IFGCTXSTAT
Service Guard Package (egate)
Interface Engines (IE)
7 clusters* (4-5 machines, one failover per cluster)
ewSITE_HL7out_MMBulk - Alerts only
ewSITE_HL7in_CHCS
ewSITE_HL7out_CHCS
W A N
W A N
Local MTF and Clinics
Remote Clinic Clinical Workstations
Second + Third Logon Attempt
Single Sign-On (Snareworks 5.0)
Second + Third Logon Attempt
First Logon Attempt
First Logon Attempt
Snareworks 5.0 Replication
MTF
Clinical Workstation (CWS)
Order Entry
Order Entry
Local Cache Traffic
LSO - PSS (Local Security Object)
Local Cache Server (NT)
Oracle ICD
Enosus CM
C++ w/ ActiveX adapter
Enosus M-adapter [DSM database, etc delivery system]
Mobjects
GIS Direct Call
Legacy CHCS
CHCS II Transmitter
CHCS II Receiver
v8.63
07/28/06
(c) NGIT

ServiceGuard Clusters
CDR: ugunhs02: Superdomewith 128 CPU/512GB RAM
gusdmm01: Superdome with 128 CPU/512GB RAM
IEs, IE FEPs, LGS FEPs, CWS FEPs = HP 2400 Class with
2 CPU/4GB RAM or 4 CPU/12 GB RAM

Key:
EMSS: Enterprise Master Security Server
PSS: Primary Security Server
* Subject to change

Figure 6. AHLTA Architecture and Data Flow.



Note: Each application (CHCS, PGUI, Citrix, TOL, etc.) has 6 servers, one server for each time zone that has a USCG clinic, i.e. East, Puerto Rico, Central, Pacific, Alaska, and Hawaii.

Figure 7. Coast Guard Connection Scheme.